APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/558,848	09/28/2006	James F. Riordan	CH920030006US1	7159

68168 7590 02/02/2009		

MICHAEL BUCHENHORNER, P.A.
8540 SW 83 STREET
SUITE 100
MIAMI, FL 33143

EXAMINER
WRIGHT, BRYAN F

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
02/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

michael@buchenhorner.com
ana@buchenhorner.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/558,848	RIORDAN, JAMES F.
	Examiner	Art Unit
	BRYAN WRIGHT	2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>20 November 2008</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>25-30</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>25-30</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

FINAL ACTION

1.   Claims 1-24 are canceled and Claims 25-30 are added in Amendment 11/20/08.

Claims 25-30 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 25-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Cohen et al. (US Patent Publication No. 2004/0148521 and Cohen hereinafter) in view

of Copeland (US Patent No. 7,290,283), further in view of Ricciulli (US Patent No.

6,473,405).

3.   As to claim 25, Cohen teaches a method for detecting attacks on a data

communications network, the method comprising:

using an intrusion detection sensor (e.g., IR) comprising intrusion detection code

for: monitoring data traffic on the network comprising a first group of addresses

assigned to known users (i.e., ... teaches 2 Data Type of Traffic Traffic Detected at IR

Direction or similar device Action Taken From North Authorized systems Traffic

directed South to have (IPs) using those services rendered authorized services (ports)

Unauthorized Traffic handled based on the systems or deception configuration

authorized systems using unauthorized services From South Authorized systems

Traffic forwarded to (IPs) rendering authorized requesters authorized (e.g. authorized

IP services (ports) addresses) from North Unauthorized Traffic handled based on

systems or the deception authorized configuration [par. 120]), and a second group of

addresses that are not assigned to the known users (i.e., ... teaches Unauthorized

Traffic handled based on systems or the deception authorized configuration. ...

teaches a systems using unauthorized services From East Traffic is directed North,

South, or West, depending on the address information associated with the deception

operation in use From West Traffic being deceived and sent to the West for that

purpose has return traffic returned to the interface it came from From Traffic from

Traffic is forwarded to a Control authorized IP secure shell session on the addresses

and IR to allow control to be ports to carried out authorized IP addresses and ports

All other traffic is ignored [par. 120]);

identifying an address belonging to the second group of addresses (i.e., ...

teaches if it has been identified that TCP traffic from 10.2.3.4 to 10.2.3.5 on South is not

authorized, the IR can cause attempted traffic of this sort in the South network to fail to

operate correctly. In other words, while an IR according to specific embodiments of the

invention may not do as well at protecting insiders from other insiders as it will for

protecting insiders from outsiders [par. 122]);

spoofing a reply to a request associated with the identified address in order to

detect data indicative of an attack (i.e., ... teaches spoofing is accomplished by in

essence changing the source and destination fields by an offset. For example, an IR

can be configured to translate a whole class B address space into another class B

address space by offsetting all of the addresses by the difference between the two class

B address spaces. From 10.2.*.* to 10.25.*.*, the translation is to add 23 to the class B

field of the address space [par. 101]);

listening for a response to the spoofing (i.e., … teaches an ssh server is

configured to listen on port 976 on the loopback interface, even though there is no real

IP address on the IR [par. 227]);

determining from the response that the request is suspicious [par. 38];

generating an alert signal instructing a router to reroute the data traffic originating

at the address assigned to the system transmitting the suspicious request to a

disinfection address on the network (i.e., … teaches reverser takes responses from that

redirected destination and undoes the redirection for return packets so that they go back

to the sender as if they came from the IP address they thought they sent the original

packets to [par. 91]);

Cohen does not teach:

sending an alert message to the disinfection address, wherein said alert

message comprises attack identity data;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Cohen as introduced by Copeland. Copeland

discloses:

sending an alert message to the disinfection address, wherein said alert

message comprises attack identity data (to transmit an alert message containing attack

identity data [col. 22, lines 55-60]);

Therefore, given the teachings of Copeland, a person having ordinary skill in the art at

the time of the invention would have recognized the desirability and advantage of

modifying Cohen by employing the well known features of transmitting an alert message

containing attack identity data disclosed above by Copeland, for which network intrusion

analysis will be enhanced [col. 22, lines 55-60].

Cohen in view of Copeland does not teach:

and billing an entity for execution of at least one of the method steps, the charge

being billed determined in dependence of one of:

a size of the network, a number of the second group of the addresses monitored,

a number of the first group of the addresses monitored, a volume of the data traffic

inspected, a number of attacks identified, a number of the alert messages generated, a

signature of the identified attack, a volume of rerouted data traffic, a degree of network

security achieved, and a turnover of said entity.

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Cohen in view of Copeland as introduced by

Ricciulli. Ricciulli discloses:

and billing an entity for execution of at least one of the method steps, the charge

being billed determined in dependence of one of:

a size of the network, a number of the second group of the addresses monitored,

a number of the first group of the addresses monitored, a volume of the data traffic

inspected, a number of attacks identified, a number of the alert messages generated, a

signature of the identified attack, a volume of rerouted data traffic, a degree of network

security achieved, and a turnover of said entity (for purposes of billing for security

relative and network traffic routing function Ricciulli provides the capability to provide

cost analysis for pertinent security and network traffic control functions as prescribed by

Cohen in view Copeland [Ricciulli; abstract]. Both Cohen in view Copeland and Ricciulli

provides robust and scalable systems as such warranting the desirability to combine

Cohen in view Copeland and Ricciulli to provide billing for the execution of process

steps relative to security and network traffic control).

Therefore, given the teachings of Ricciulli, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Cohen in view Copeland by employing the well known features of network security and traffic control cost determination disclosed above by Ricciulli, for which network security and traffic control will be enhanced [Ricciulli; abstract].

4.   As to claim 26, Cohen teaches a method where the step of determining from the response comprises receiving no response within a specified time period (i.e., … teaches comparing an incoming datagram to a set of stimulus/response rules, each rule providing a particular action to be performed regarding a datagram that matches that rule's associated stimulus [claim 20]).

5.   As to claim 27, Cohen teaches a method of claim 25 wherein the step of determining from the response comprises receiving the response within a specified time period and comparing said response (e.g.. packet) to the attack identity data stored (i.e., matching rule) in memory, wherein the memory stores signatures identifying known attacks (i.e., … teaches comparing an incoming datagram against one or more rules to determine a matching rule for a particular datagram. [claim 19] … further teaches comparing an incoming datagram to a set of stimulus/response rules, each rule providing a particular action to be performed regarding a datagram that matches that rule's associated stimulus [claim 20]).

6.   As to claim 28, Cohen teaches a method where sending the alert message (i.e.,

response) comprising the attack identity data comprises sending data indicative of

signatures (i.e., fingerprints) of identified known attacks (i.e., ... teaches IR is designed

to utilize OS fingerprints from the Xprobe2 fingerprints file which can be obtain from

Xprobe2 in order to spoof ICMP responses to Xprobe2 scans [par. 272]).

7.   As to claim 29, Cohen teaches a method where the monitoring step comprises

listening only for the data traffic directed to the second group of addresses [par. 272].

8.   Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen

in view of Copeland.

9.   As to claim 30, Cohen teaches a method comprising steps of: using a disinfection

server for:

       receiving an alert message sent from an intrusion detection sensor (i.e., ...

teaches reverser takes responses from that redirected destination and undoes the

redirection for return packets so that they go back to the sender as if they came from

the IP address they thought they sent the original packets to [par. 91]),

       sending a warning message (e.g., response) to an address assigned to the

system, wherein said warning message comprises program code for eliminating the

network attack when executed by the system originating the data indicative of the attack

(i.e., ... teaches a command transmits a packet back to its sender while flipping one or

more of the sending and receiving MAC, IP, and PORT values of the packet. Generally,

the packet is transmitted out of the same interface where it arrived and thus this

command can be used on a logic module according to specific embodiments of the

invention that has only one network interface. This type of response can cause an

attacker to potentially connect back to their own computer system and possible divert

any malicious action back at the attackers own computer system [par. 88]);

supporting an entity in handling of the detected attack by one of providing

instructions for use of, assistance in executing (e.g., counter action), and execution of

disinfection program code (i.e., ... teaches a one or more distinct deceptive responses

can be provided to an incoming packet. ... further teaches FIG. 6 is a flowchart

illustrating a general method for providing counter actions against attacking information

systems according to embodiments of the present invention [par. 86]);

and providing a report to the entity containing information related to one of alert,

disinfection, rerouting, logging, and discarding of data traffic in the context of the

detected attack (i.e., ... teaches logs to syslog or other file or logging method or system

for capture and analysis by remote devices [par. 260])

Cohen does not teach:

said alert message comprising data indicative of signatures of identified known

attacks for identifying a system originating data indicative of a network attack;

However, these features are well known in the art and would have been an obvious

modification of the system disclosed by Cohen as introduced by Copeland. Copeland

discloses:

said alert message comprising data indicative of signatures of identified known

attacks for identifying a system originating data indicative of a network attack (to

transmit an alert message containing attack identity data [col. 22, lines 55-60]);

Therefore, given the teachings of Copeland, a person having ordinary skill in the art at

the time of the invention would have recognized the desirability and advantage of

modifying Cohen by employing the well known features of transmitting an alert message

containing attack identity data disclosed above by Copeland, for which network intrusion

analysis will be enhanced [col. 22, lines 55-60].

Response to Arguments

Applicant's arguments with respect to claims 25-30 have been considered but are

moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-

3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435